The Gröbner Basis of the
Ideal of Vanishing Polynomials

Gert-Martin Greuel,[*] Frank Seelisch,[†] Oliver Wienand

January 2009

Abstract

We construct an explicit minimal strong Gröbner basis of the ideal of vanishing polynomials in the polynomial ring over $\mathbb{Z}/m$ for $m \geq 2$. The proof is done in a purely combinatorial way. It is a remarkable fact that the constructed Gröbner basis is independent of the monomial order and that the set of leading terms of the constructed Gröbner basis is unique, up to multiplication by units. We also present a fast algorithm to compute reduced normal forms, and furthermore, we give a recursive algorithm for building a Gröbner basis in $\mathbb{Z}/m[x_1, x_2, \ldots, x_n]$ along the prime factorization of m. The obtained results are not only of mathematical interest but have immediate applications in formal verification of data paths for microelectronic systems-on-chip.

1   Introduction

Although the basic properties of Gröbner bases in polynomial rings over a ring C are well-known (see [1]), they have not been studied very much, mainly because they were considered as academic, in contrast to the case where the ground ring C is a field. Recently however, Gröbner basis techniques in polynomial rings over $C = \mathbb{Z}/m$ (in particular $\mathbb{Z}/2^k$) have attracted some attention due to their potential applications to proving correctness of data paths in system-on-chip design (cf. e.g. [7],[8], [12]).

When the underlying ring C has only finitely many elements, then there exist polynomials in $C[x_1, x_2, \ldots, x_n]$ which evaluate to zero for all $(a_1, a_2, \ldots, a_n) \in C^n$, called vanishing polynomials. Thus, any polynomial function $\widetilde{f} : C^n \to C$ given by an arbitrary element $f \in C[x_1, x_2, \ldots, x_n]$, will have many alternative representations in $C[x_1, x_2, \ldots, x_n]$, as $\widetilde{f} = \widetilde{f + g}$, for all g that constantly vanish on C^n. All vanishing polynomials constitute an ideal I_0.

[*]Department of Mathematics, Working Group *Algebra, Geometry, and Computer Algebra*, University of Kaiserslautern, Germany. Email: greuel@mathematik.uni-kl.de.

[†]Email: seelisch@mathematik.uni-kl.de.

In the applications mentioned above, not the polynomials but only the polynomial functions are of interest. Thus, if we want to apply algebraic methods we need to be able to efficiently compute normal forms of polynomials with respect to a Gröbner basis of I_0. In the presented paper, we set the theoretical ground and provide fast algorithms for doing these computations.

From a mathematical point of view, $I_0 \subset \mathbb{Z}/m[x_1, x_2, \ldots, x_n]$ has some interesting properties. In this paper, we will give an explicit minimal strong Gröbner basis G_m for I_0. As will turn out, G_m is a Gröbner basis with respect to *every* global monomial order. Moreover, we will show for any alternative minimal strong Gröbner basis G of $I_0 \subset \mathbb{Z}/m[x_1, x_2, \ldots, x_n]$ that the sets of leading terms of G_m and G are the same up to multiplication by units. This is remarkable, since the ring $\mathbb{Z}/m$ has zero divisors. In general, the leading terms of two minimal strong Gröbner bases of an ideal $I \subset C[x_1, x_2, \ldots, x_n]$ need not be related by a unit but only by some element of C. We will prove both properties and show also that in general all minimal strong Gröbner bases of an arbitrary ideal $I \subset C[x_1, x_2, \ldots, x_n]$ have the same number of elements.

From a practical point of view, as mentioned above, engineering tasks involving the computation of Gröbner bases over finite rings will often need to deal with vanishing polynomials. This is due to the fact that normally the elements of a Gröbner basis G will be used to decide the consistency of a mathematical model. And typically, such a check involves the question whether the set of zeros of all polynomials $f \in G$ coincides with the set of all feasible input-output vectors of the modelled artifact; see also [7]. Our interest was specifically spurred by a cooperation with the local Electronic Design Automation Group in which we use Gröbner bases to formally verify chip designs. More precisely, a given verification task is translated into a polynomial ideal in $\mathbb{Z}/2^k$, where typically $k = 32$ or $k = 64$; cf. [11]. For the special case of polynomial datapath verification we also refer to [12] in which it was shown that the Gröbner basis approach proves tractable for industrial applications where standard property checking techniques failed.

This paper is organized as follows. Section 2 briefly recalls the basic concepts from the theory of polynomial rings and Gröbner bases needed later. Section 3 starts by presenting canonical members of the ideal of vanishing polynomials $I_0 \subset \mathbb{Z}/m[x_1, x_2, \ldots, x_n]$. Next we show that the leading term of any given vanishing polynomial is divisible by the leading term of an appropriate canonical member. This relation enables us to finally construct an explicit minimal strong Gröbner basis G_m of $I_0 \subset \mathbb{Z}/m[x_1, x_2, \ldots, x_n]$. We also show that the size of G_m is of polynomial order of degree k in the number of variables n, when we are in the practically relevant case $m = 2^k$.

The theoretical results are followed by algorithms for computing reduced normal forms with respect to the constructed basis, and for recursively computing a Gröbner basis of $I_0 \subset \mathbb{Z}/m[x_1, x_2, \ldots, x_n]$ along the prime factorization of m. The normal form algorithm has been implemented in the computer algebra system SINGULAR [3] and successfully applied, [12].

2 Preliminaries

Let C be a commutative, noetherian ring with 1, and $C[\mathbf{x}] := C[x_1, x_2, \ldots, x_n]$ a multivariate polynomial ring over C, where $n \geq 1$. For any multi-index $\alpha = (\alpha_1, \ldots, \alpha_n) \in \{0, 1, 2, \ldots\}^n$, a product of variables $\mathbf{x}^\alpha := x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ is called a monomial, and a product $a \cdot \mathbf{x}^\alpha$ with $a \in C$ is called a term.

Given two multi-indices $\alpha = (\alpha_1, \ldots, \alpha_n), \beta = (\beta_1, \ldots, \beta_n)$, we define $\alpha \pm \beta := (\alpha_1 \pm \beta_1, \ldots, \alpha_n \pm \beta_n)$. We may compare α and β according to the predicate $\alpha \preceq \beta :\Leftrightarrow \forall i \in \{1, \ldots, n\} : \alpha_i \leq \beta_i$, and similarly $\alpha \prec \beta :\Leftrightarrow \alpha \preceq \beta \wedge \alpha \neq \beta$. For $\alpha = (\alpha_1, \ldots, \alpha_n) \in \{0, 1, 2, \ldots\}^n$, we write $\alpha! := \alpha_1! \cdots \alpha_n!$, and $|\alpha| := \alpha_1 + \ldots + \alpha_n$.

Moreover, we require the polynomial ring $C[\mathbf{x}]$ to be equipped with a global monomial order $<$, i.e., $<$ is a well-order on the set of monomials and satisfies $\mathbf{x}^\alpha > \mathbf{x}^\beta \Rightarrow \mathbf{x}^{\alpha+\gamma} > \mathbf{x}^{\beta+\gamma}$ for all $\alpha, \beta, \gamma \in \{0, 1, 2, \ldots\}^n$. Then $<$ refines the partial order $\prec$.

Since we are going to work with divisibility in $\mathbb{Z}/m[x_1, x_2, \ldots, x_n]$, we need to distinguish between divisibility in $\mathbb{Z}/m$ and in $\mathbb{Z}$. We set $a\big|_{\mathbb{z}} b :\Leftrightarrow \exists k \in \mathbb{Z} : b = a \cdot k$ and $a\big|_{m} b :\Leftrightarrow \exists k \in \mathbb{Z} : m\big|_{\mathbb{z}} (b - a \cdot k)$, that is, b and $a \cdot k$ represent the same residue class in $\mathbb{Z}/m$. For two monomials $a\mathbf{x}^\alpha, b\mathbf{x}^\beta$, we say that $a\mathbf{x}^\alpha$ divides $b\mathbf{x}^\beta$, if $a\big|_{m} b \wedge \alpha \preceq \beta$. We then write $a\mathbf{x}^\alpha | b\mathbf{x}^\beta$, using the ordinary symbol.

Let $f = a_0 \cdot \mathbf{x}^{\alpha^{(0)}} + \cdots + a_k \cdot \mathbf{x}^{\alpha^{(k)}}$ be a polynomial in $C[x_1, x_2, \ldots, x_n]$ with $a_i \neq 0$ for $0 \leq i \leq k$, and $x^{\alpha^{(0)}} > x^{\alpha^{(1)}} > \cdots > x^{\alpha^{(k)}}$. We use the following notation:

$$\deg(f) = \max\{|\alpha^{(i)}| \mid 0 \leq i \leq k\} \qquad \text{total degree of } f,$$

$$\mathrm{LT}(f) = a_0 \cdot \mathbf{x}^{\alpha^{(0)}} \qquad \text{leading term of } f,$$

$$\mathrm{LM}(f) = \mathbf{x}^{\alpha^{(0)}} \qquad \text{leading monomial of } f,$$

$$\mathrm{LC}(f) = a_0 \qquad \text{leading coefficient of } f,$$

$$\mathrm{L}(A) = \langle \mathrm{LT}(f) \mid f \in A \rangle_{C[x_1, x_2, \ldots, x_n]} \quad \text{leading ideal of } A,$$

$$\text{for } A \subset C[x_1, x_2, \ldots, x_n],\ A \neq \emptyset.$$

For an ideal $I \subset C[x_1, x_2, \ldots, x_n]$ a finite set $G \subset C[x_1, x_2, \ldots, x_n]$ is called a **Gröbner basis** of I if

$$G \subset I, \text{ and } \mathrm{L}(I) = \mathrm{L}(G).$$

That is, G is a Gröbner basis, if the leading terms of G generate the leading ideal of I. Note that in general, all defined objects depend on the chosen monomial order. Especially, a set G may be a Gröbner basis only with respect to a certain monomial order. We also remind the reader that with the given definition, G already generates I, cf. [1].

G is furthermore called a **strong Gröbner basis** if for any $f \in I \backslash \{0\}$ there exists a polynomial $g \in G$ satisfying $\mathrm{LT}(g) \mid \mathrm{LT}(f)$. A strong Gröbner basis G is called **minimal strong** if $\mathrm{LT}(g_1) \nmid \mathrm{LT}(g_2)$ for all distinct $g_1, g_2 \in G$. It is a well-known fact that a strong Gröbner basis can always be constructed from a

given Gröbner basis when C is a principal ideal domain, see e.g. [1].

Note that if C is a field, any non-zero coefficient of a term is invertible in C, and thus $\mathrm{L}\,(A) = \langle \mathrm{LM}\,(f) \mid f \in A \rangle$. It is easy to verify that in this case every Gröbner basis is a strong Gröbner basis. As the following example shows, this does in general not hold when C is a ring:

Example 2.1. *Consider $C := \mathbb{Z}/6$, and the polynomial ring $C[x]$ with one variable. Then $G := \{2x, 3x\}$ is a Gröbner basis of the ideal $I := \langle x \rangle$. But since neither $2x$ nor $3x$ divide x, G is not a strong Gröbner basis.*

We shall now capture the central notions of this paper.

Definition 2.2. *To any polynomial $f \in C[x_1, x_2, \ldots, x_n]$ we associate the polynomial function $\widetilde{f} : C^n \to C$, $(c_1, c_2, \ldots, c_n) \mapsto f(c_1, c_2, \ldots, c_n)$. We call f a* **vanishing polynomial** *if the function $\widetilde{f}$ is identically zero.*

The set $I_0 = \{f \in C[x_1, x_2, \ldots, x_n] \mid f$ is a vanishing polynomial$\}$ is obviously an ideal in $C[x_1, x_2, \ldots, x_n]$, called the **ideal of vanishing polynomials***.*

3 A Minimal Strong Gröbner Basis of the Ideal of Vanishing Polynomials

3.1 The Ideal of Vanishing Polynomials

From now on let the coefficient ring be $C = \mathbb{Z}/m$, where $m \geq 2$, except stated otherwise. The following results were inspired by the work of Singmaster [9], Kempner [6], Halbeisen, Hungerbühler, and Läuchli [4], and Hungerbühler and Specker [5]. Already in Lemma 5 of [6], a univariate version of the following lemma was proven. Theorem 7 of [4] restated this result, and [5] came up with a generalization to multivariate polynomial rings over $\mathbb{Z}/m$.

Lemma 3.1. *Let $a \in \mathbb{Z}$ and $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}_0^n$ such that $m|_{\mathbb{Z}} a\alpha!$. Then*

$$p_{\alpha,a} := a \prod_{i=1}^{n} \prod_{l=1}^{\alpha_i} (x_i - l) \in \mathbb{Z}/m[x_1, \ldots, x_n]$$

is a vanishing polynomial.

Proof. Fix an arbitrary point $(c_1, c_2, \ldots, c_n) \in C^n$. Then $p_{\alpha,a}(c_1, c_2, \ldots, c_n)$ contains, for all i, by definition the α_i successive factors $c_i - 1, c_i - 2, \ldots, c_i - \alpha_i$. Independent of the value of c_i, these contain all factors from 2 up to α_i. Therefore, $\alpha_i!$ divides $p_{\alpha,a}(c_1, c_2, \ldots, c_n)$, for all i. By combining these results, it follows immediately that $a\alpha_1! \cdots \alpha_n!$ divides $p_{\alpha,a}(c_1, c_2, \ldots, c_n)$. With $m|_{\mathbb{Z}} a\alpha!$ this yields $p_{\alpha,a}(c_1, c_2, \ldots, c_n) = 0$ modulo m. $\qquad\square$

Let us now take a closer look at an arbitrary vanishing polynomial:

Lemma 3.2. *Let $f \in I_0 \subset \mathbb{Z}/m[x_1, x_2, \ldots, x_n]$ be an arbitrary vanishing polynomial with $\mathrm{LT}\,(f) = b\mathbf{x}^\beta$. Then $m|_{\mathbb{Z}} b\beta!$.*

For the proof we use some of the ideas introduced in [5], which are based on the notion of partial differences in the multivariate setting. Already Carlitz used partial differences in the univariate case, see [2], to give a necessary and sufficient condition for a function f over $\mathbb{Z}/p^k$ to be a polynomial function.[1]

Proof. Let $C[x_1,\ldots,x_n]$ denote an arbitrary polynomial ring over $n \geq 1$ variables, and let $h \in C[\mathbf{x}]$ be a polynomial. Then we may define the ith partial difference

$$\nabla_i h := h(x_1,\ldots,x_{i-1},x_i+1,x_{i+1},\ldots,x_n) - h(x_1,\ldots,x_{i-1},x_i,x_{i+1},\ldots,x_n),$$

for $1 \leq i \leq n$. Note that ∇_i is a linear operator.

Now we can define the successive application of the operator by

$$\nabla_i^0 h := h, \quad \text{and} \quad \nabla_i^{k+1} h := \nabla_i \nabla_i^k h, \text{ for } k \geq 0.$$

(For n = 1, $\nabla_1^k h$ coincides with Carlitz' $\triangle^k h$; see [2].)

Since obviously, $\nabla_i \nabla_j h = h(x_1,\ldots,x_i+1,\ldots,x_j+1,\ldots,x_n) - h(x_1,\ldots, x_i+1,\ldots,x_n) - h(x_1,\ldots,x_j+1,\ldots,x_n) + h(x_1,\ldots,x_n) = \nabla_j \nabla_i h$, for all $i,j \in \{1,\ldots,n\}$, we can extend the operator to arbitrary multi-indices, that is, with $\alpha = (\alpha_1,\ldots,\alpha_n) \in \{0,1,2,\ldots\}^n$, the term

$$\nabla^\alpha h := \nabla_1^{\alpha_1} \nabla_2^{\alpha_2} \ldots \nabla_n^{\alpha_n} h$$

is independent from the order of application of the ∇_i operators and hence well-defined.

Let us consider the difference $(x_i+1)^k - x_i^k = k \cdot x_i^{k-1} + g(x_i)$, where g consists of lower terms only, that is, $\deg(g) < k - 1$. A simple induction shows that $\nabla_i^k x_i^k = k!$ and $\nabla_i^j x_i^k = 0$, whenever $j > k$. Let now $a\mathbf{x}^\alpha := \mathrm{LT}(h)$ denote the leading term. Then, mainly due to the linearity of the ∇_i operators, it is easy to see that the previous facts can be further abstracted to the general statements

$$\nabla^\alpha h = a\alpha! \quad \text{and} \quad \nabla^\beta h = 0, \text{ for all } \beta \succ \alpha.$$

We apply the first equation to the vanishing polynomial f over the ring $\mathbb{Z}/m$: With f also $\nabla^\beta f = b\beta!$ must be a vanishing polynomial, by construction. But this implies $b\beta! = 0$ modulo m. $\qquad\square$

3.2 A Minimal Strong Gröbner Basis of I_0

The above lemmas suggest to consider the set of all polynomials $p_{\alpha,a}$ for which neither α nor a can be replaced by a smaller multi-index or element of $\mathbb{Z}/m$, respectively, without loosing the condition $m|_\mathbb{Z} a\alpha!$. (This minimality of α has been inspired by the so-called Smarandache function which maps m to $min\{k \in \mathbb{N} \mid m|_\mathbb{Z} k!\}$. This function played a role in previous works which studied the univariate case, and had been named after F. Smarandache, see [10],

---

[1]I.e., $f(a) = g(a) \bmod p^k$, for all $a \in \mathbb{Z}/p^k$ and some polynomial $g \in \mathbb{Z}/p^k[x]$.

although the idea had been introduced earlier by Kempner in Definition 1 of
[6].) We thus define

$$S_m := \{\, (\alpha, a) \mid 1 \leq a < m,\ a|_{\mathbb{Z}} m,\ \alpha \in \mathbb{N}_0^n,\ m|_{\mathbb{Z}} a\alpha!,$$
$$\forall\, \beta \prec \alpha :\ m \nmid_{\mathbb{Z}} a\beta!,$$
$$\forall\, b < a,\ b|_{\mathbb{Z}} a :\ m \nmid_{\mathbb{Z}} b\alpha!\,\},$$
$$G_m := \{\, p_{\alpha,a} \mid (\alpha, a) \in S_m \,\}.$$

Note that, according to Lemma 3.1, all polynomials in G_m will still be elements
of I_0. And by Lemma 3.2, we can hope to have constructed a strong Gröbner
basis.

Theorem 3.3. *Let $m \geq 2$ and $n \geq 1$ be arbitrary integers. With the above
notations, G_m is a minimal strong Gröbner basis of the ideal of vanishing poly-
nomials $I_0 \subset \mathbb{Z}/m[x_1, x_2, \ldots, x_n]$, independent of the global monomial order.*

Before we prove the theorem, let us take a look at an example.

Example 3.4. *Let $m = q_1 \cdot q_2 \cdots q_k$ be a product of $k \geq 1$ mutually distinct
primes, and $n \geq 1$ arbitrary. We assume $q_1 < q_2 < \ldots < q_k$. Then we can
immediately write down all elements of G_m:*

$$(x_i - 1)(x_i - 2) \cdots (x_i - q_k),$$
$$q_k \cdot (x_i - 1)(x_i - 2) \cdots (x_i - q_{k-1}),$$
$$q_k \cdot q_{k-1} \cdot (x_i - 1)(x_i - 2) \cdots (x_i - q_{k-2}),$$
$$\cdots$$
$$q_k \cdot q_{k-1} \cdots q_2 \cdot (x_i - 1)(x_i - 2) \cdots (x_i - q_1),$$

in each row for all $i \in \{1, 2, \ldots, n\}$.

Note that the first type of polynomial is in G_m, as $q_k!$ already contains all
q_j, thus $m|_{\mathbb{Z}} q_k!$. Also, we need to have all q_k polynomial factors since, for all
$r < q_k$, $q_k \nmid_{\mathbb{Z}} r!$, i.e. $m \nmid_{\mathbb{Z}} r!$. For the following polynomials, the argument is
similar. Moreover, it is easy to see that we do not have elements in G_m involving
two or more variables, and the presented polynomials are all elements of G_m.
In this special case $|G_m| = k \cdot n$, and the maximal degree is q_k. This means that
the size of the basis is only linear in the number of variables.
For the case $k = 1$, $\mathbb{Z}/q_1$ is a field, and we obtain only the n polynomials in the
top row, which are well-known for this case.
We now prove the theorem:

Proof. Let us fix $m \geq 2$, the number of variables $n \geq 1$, and an arbitrary global
monomial order. We first show that G_m is indeed a Gröbner basis of I_0. To this
end, it suffices to show that (i) S_m and hence G_m is a finite set, (ii) $G_m \subset I_0$,
and (iii) $\mathrm{L}\,(I_0) \subset \mathrm{L}\,(G_m)$, since (ii) implies the other inclusion $\mathrm{L}\,(G_m) \subset \mathrm{L}\,(I_0)$.
(i) Since $(\alpha, a) \in S_m$ implies $\alpha \preceq (m, m, \ldots, m)$, the set is clearly finite.

(ii) G_m consists of polynomials $p_{\alpha,a}$ with $m|_{\mathbb{z}} a\alpha!$. Then $G_m \subset I_0$ by Lemma 3.1.

(iii) Let $f \in \mathrm{L}(I_0)$ be arbitrary. Then there exist some integer $N \geq 1$, $h_i \in \mathbb{Z}/(m)[x_1, x_2, \ldots, x_n]$ and $f_i \in I_0, 1 \leq i \leq N$, such that

$$f = \sum_{i=1}^{N} h_i \cdot \mathrm{LT}(f_i).$$

Writing $a_i \mathbf{x}^{\alpha^{(i)}} := \mathrm{LT}(f_i)$, we obtain $m|_{\mathbb{z}} a_i \alpha^{(i)}!$ from Lemma 3.2. Now either $(\alpha^{(i)}, a_i)$ is already an element of S_m. Or we can replace a_i by some $b_i|_{\mathbb{z}} a_i$ and/or $\alpha^{(i)}$ by some $\beta^{(i)} \preceq \alpha^{(i)}$ such that $(\beta^{(i)}, b_i) \in S_m$. We can subsume both cases in saying that, for each $i \in \{1, 2, \ldots, N\}$, there is some $(\beta^{(i)}, b_i) \in S_m$ such that $b_i \mathbf{x}^{\beta^{(i)}} | \mathrm{LT}(f_i)$. With appropriate polynomials $g_i, 1 \leq i \leq N$, this amounts to

$$f = \sum_{i=1}^{N} h_i \cdot g_i \cdot \mathrm{LT}\left(p_{\beta^{(i)}, b_i}\right),$$

i.e., $f \in \mathrm{L}(G_m)$.

Next, let $f \in I_0$. Then, with the same argument as for the f_i above, there exists a $p_{\gamma,c} \in G_m$ such that $\mathrm{LT}(p_{\gamma,c}) | \mathrm{LT}(f)$. This shows that G_m is a strong Gröbner basis.

It remains to show that G_m is minimal. To this end, pick two pairs $(\alpha, a), (\beta, b) \in S_m$ such that $a\mathbf{x}^\alpha | b\mathbf{x}^\beta$. Then $a|_m b$, $a|_{\mathbb{z}} m$, $b|_{\mathbb{z}} m$, and $\alpha \preceq \beta$. We need to prove that $a = b$ and $\alpha = \beta$. Computing in $\mathbb{Z}$, take a prime factor q of b and $k \geq 1$ maximal such that $q^k|_{\mathbb{z}} b$. Suppose $q^k \nmid_{\mathbb{z}} a$. Then $a\alpha!$ would have at least one less factor q in its prime factorization than $b\alpha!$. But since $m|_{\mathbb{z}} a\alpha!$, we then had $m|_{\mathbb{z}} b/q \cdot \alpha!|_{\mathbb{z}} b/q \cdot \beta!$, and b would not be minimal in $(\beta, b) \in S_m$. We conclude that $b|_{\mathbb{z}} a$. We write this as $a = d \cdot b$ for some $d|_{\mathbb{z}} m$. Now $a|_m b$, that is, $m|_{\mathbb{z}} a \cdot c - b$ for some c. Putting things together we get $bd = a|_{\mathbb{z}} m|_{\mathbb{z}} bcd - b = b(cd - 1)$. Hence $d|_{\mathbb{z}} (cd - 1)$ which can only hold for $d = 1$, implying $a = b$. But then we must also have $\alpha = \beta$, since otherwise β would not be minimal in $(\beta, b) \in S_m$. $\square$

We now show that leading terms of minimal strong Gröbner bases of $I_0 \subset \mathbb{Z}/m[x_1, x_2, \ldots, x_n]$ are unique, up to multiplication by units of $\mathbb{Z}/m$. We prove this result as a consequence of a more general statement for ideals over arbitrary commutative rings with 1 that has, to our knowledge, not been stated before. (Note the similar statement in the field case; see e.g. Proposition 1.8.4 in [1].)

Theorem 3.5. *a) Let G, F be two minimal strong Gröbner basis of an arbitrary ideal $I \subset C[x_1, x_2, \ldots, x_n]$, where C is any commutative ring with 1. Then $|G| = |F|$, and the sets of leading terms in G and F coincide up to multiplication by elements of C, i.e.,*

$$\forall\, g \in G \ \exists\, f \in F \ \exists\, c \in C \ \ \mathrm{LT}(g) = c \cdot \mathrm{LT}(f). \quad (*)$$

b) In the case of $C = \mathbb{Z}/m$ and $I = I_0$, the ring elements c in $(*)$ can be chosen to be units of $\mathbb{Z}/m$.

Note that the second statement holds for any ideal, if the ring C is a domain.

Proof. a) Starting with the proof of $(*)$, we pick any $g \in G \subset I$. Then, by strongness of F, there is some $f \in F$ such that $\mathrm{LT}\,(f) \,|\, \mathrm{LT}\,(g)$. Vice versa, by strongness of G, there must be some $g' \in G$ such that $\mathrm{LT}\,(g') \,|\, \mathrm{LT}\,(f)$. Therefore, $\mathrm{LT}\,(g') \,|\, \mathrm{LT}\,(f) \,|\, \mathrm{LT}\,(g)$, which implies $g = g'$, by minimality of G. But then the leading monomials $\mathrm{LM}\,(f)$ and $\mathrm{LM}\,(g)$ must also coincide, yielding the desired relation between $\mathrm{LT}\,(f)$ and $\mathrm{LT}\,(g)$.

Similar to the previous argument, it is easy to see that no two distinct leading terms in F can fulfil a relation $(*)$ with the same leading term in G, and vice versa. This implies the equality $|\{\mathrm{LT}\,(g) \mid g \in G\}| = |\{\mathrm{LT}\,(f) \mid f \in F\}|$ which clearly amounts to $|G| = |F|$, by the minimality of G and F.

b) We first choose $G = G_m$ to be the explicitly given Gröbner basis, and F any other minimal strong Gröbner basis of $I_0 \subset \mathbb{Z}/m[x_1, x_2, \ldots, x_n]$. Consider a relation as in $(*)$, i.e., $b \cdot \mathbf{x}^\beta = c \cdot a \cdot \mathbf{x}^\alpha$, where $(\beta, b) \in S_m$ and $a \cdot \mathbf{x}^\alpha$ denotes the leading term of some $f \in F$. Then $b = a \cdot c \bmod m$, in other words $m|_{\mathbb{z}}\, ac - b$. Now let $\tilde{a} := \gcd\,(a, m)$ be the maximum portion of a that divides m, that is, $a = \tilde{a} \cdot u$, where $\gcd\,(u, m) = 1$ which is equivalent to u being a unit in $\mathbb{Z}/m$. Since $\tilde{a}|_{\mathbb{z}}\, m|_{\mathbb{z}}\, ac - b$, we obtain $\tilde{a}|_{\mathbb{z}}\, b$.

We want to show $\tilde{a} = b$, so for a contradiction let us assume $\tilde{a} < b$. $f \in F \subset I_0$ implies $m|_{\mathbb{z}}\, a\alpha!$ by Lemma 3.2, hence $m|_{\mathbb{z}}\, \tilde{a}\alpha! = \tilde{a}\beta!$, as the factors in $a/\tilde{a}$ do not affect divisibility by m and since obviously $\alpha = \beta$. But this means that we could replace b by the smaller $\tilde{a}$ and still preserve the condition $m|_{\mathbb{z}}\, \tilde{a}\beta!$. This contradicts the minimality of b in $(\beta, b) \in S_m$. Hence $\tilde{a} = b$.

We thus arrive at the claimed relation $u \cdot b\mathbf{x}^\beta = a\mathbf{x}^\alpha$, and c can be replaced by the unit $u^{-1} \in (\mathbb{Z}/m)^*$.

We have shown that we can relate the leading terms of any minimal strong Gröbner basis F of $I_0 \subset \mathbb{Z}/m[x_1, x_2, \ldots, x_n]$ to the leading terms in G_m by units. By transitivity, we can now clearly also relate the leading terms of any two minimal strong Gröbner bases by units. This concludes the proof. $\square$

Note that an arbitrary factor c, relating two leading terms, need not necessarily be a unit. For example, consider the polynomial $f(x, y) = 3(x - 1)(x - 2) \cdot (y - 1)(y - 2) \in G_{12}$. We may switch to another minimal strong Gröbner basis of $I_0 \subset \mathbb{Z}/12[x, y]$, simply by replacing $f(x, y)$ by $f'(x, y) = 9(x - 1)(x - 2) \cdot (y - 1)(y - 2)$. Note that over $\mathbb{Z}/12$ the ideals $\langle f \rangle$ and $\langle f' \rangle$ are identical. Thus, $G_m \setminus \{f\} \cup \{f'\}$ must still be a minimal strong Gröbner basis. Now obviously $\mathrm{LT}\,(f') = 3 \cdot \mathrm{LT}\,(f)$, but 3 is not a unit in $\mathbb{Z}/12$.

We point out that minimal strong Gröbner bases are in general not unique. This is due to the fact that we only consider leading terms and do not require tail reduction here. For example, in the case of the ideal I_0, we can easily modify the basis G_m and still obtain a minimal strong Gröbner basis. To this end, we may pick two elements $f, g \in G_m$ with $\mathrm{LM}\,(g) < \mathrm{LM}\,(f)$ and replace f by $f + g$.

Let us once again take a look at the complexity of G_m, that is, the size $|G_m|$ as a function of the number of variables n. The discussion that followed Example 3.4 already made clear that $|G_m|$ is only linear in n, when all prime factors

of m are mutually distinct. In the general case when $m = q_1^{e_1} \cdot q_2^{e_2} \cdots q_k^{e_k}$ with some $e_j > 1$, the construction is combinatorially more complex. However, based on the following investigation for the practically relevant case $m = q^k$, we conjecture that for fixed m the size of G_m is always of polynomial order in n. Since we are interested in the asymptotic behaviour of $|G_m|$ for large n, we may assume that n is much larger than $m = q^k$. We can decompose G_m into the disjoint union

$$G_m = \bigcup_{0 \le j < k} G_m^{(j)}, \ \text{where}$$

$$G_m^{(j)} := \{ q^j \cdot (x_i - 1) \cdots (x_i - (k-j)q) \mid 1 \le i \le n \}$$
$$\cup \{ q^j \cdot (x_{i_1} - 1) \cdots (x_{i_1} - s_1 q)(x_{i_2} - 1) \cdots (x_{i_2} - s_2 q) \mid$$
$$1 \le i_1, i_2 \le n; i_1 \ne i_2; 1 \le s_1, s_2; s_1 + s_2 = k - j \}$$
$$\cdots$$
$$\cup \{ q^j \cdot (x_{i_1} - 1) \cdots (x_{i_1} - q)(x_{i_2} - 1) \cdots (x_{i_2} - q) \cdots$$
$$(x_{i_{k-j}} - 1) \cdots (x_{i_{k-j}} - q) \mid 1 \le i_u \le n; i_u \ne i_v \text{ for } u \ne v \},$$

that is, in $G_m^{(j)}$ we have the constant coefficient q^j, and we have polynomials in 1 up to $k - j$ variables. With $h_j := |G_m^{(j)}|$, we obtain the very rough estimates

$$h_j \le n + \binom{n}{2} \cdot k^1 + \cdots + \binom{n}{k-j} \cdot k^{k-j-1} = \sum_{l=1}^{k-j} \binom{n}{l} \cdot k^{l-1} \le \binom{n}{k} \cdot k^k,$$

$$h_j \ge \binom{n}{k-j}.$$

For $h := |G_m| = \sum_{0 \le j < k} h_j$ we thus get

$$\binom{n}{k} \le \sum_{j=0}^{k-1} \binom{n}{k-j} \le h \le k \cdot \binom{n}{k} \cdot k^k = \binom{n}{k} \cdot k^{k+1},$$

and $h = |G_m|$ is of polynomial order of degree k in the number of variables n.

3.3 Computing the Reduced Normal Form of a Polynomial

After we have given a minimal strong Gröbner basis of $I_0 \subset \mathbb{Z}/m[x_1, x_2, \ldots, x_n]$, we shall now turn to computing representatives of the residue classes in $(\mathbb{Z}/m[x_1, x_2, \ldots, x_n])/I_0$. When we impose certain bounds on the coefficients of all monomials, these representatives are unique:

Proposition 3.6. *Every residue class $\bar{f} \in (\mathbb{Z}/m[x_1, x_2, \ldots, x_n])/I_0$ has a unique representative $f \in \mathbb{Z}/m[x_1, x_2, \ldots, x_n]$ of the form*

$$f = \sum_{\alpha \in \{0, 1, \ldots, m-1\}^n} a_\alpha \mathbf{x}^\alpha, \ \text{where } 0 \le a_\alpha < \frac{m}{\gcd(m, \alpha!)}, \text{ for all } \alpha.$$

Note that, whenever $m|_{\mathbb{Z}}\alpha!$, the given bound forces a_α to be zero.

Proof. Let $f \in \mathbb{Z}/m[x_1, x_2, \ldots, x_n]$ be an arbitrary polynomial. Suppose f containes a monomial $a\mathbf{x}^\alpha$ for which $a \geq c := \frac{m}{\gcd(m,\alpha!)}$. Due to division with remainder of a by c in $\mathbb{Z}$, we obtain $a = k \cdot c + r$ for some $k \in \{1, 2, \ldots\}$, and $0 \leq r < c$. Now, $m|_{\mathbb{Z}} \frac{m\alpha!}{\gcd(m,\alpha!)}$. In other words, $m|_{\mathbb{Z}} c\alpha!$, and $p_{\alpha,c} \in I_0$ by Lemma 3.1.

As a consequence, f and $f' := f - k \cdot p_{\alpha,c}$ lie in the same residue class. Moreover, the coefficient of $\mathbf{x}^\alpha$ in f' is $a - k \cdot c = r$, for which the claimed bound holds. Since we have a global order on the monomials, we need only finitely many repetitions of the presented reduction step, in order to arrive at a polynomial g which also lies in the residue class of f, and the coefficients of which all satisfy the required bound condition.

For proving uniqueness of the constructed representative, assume we have two representatives f_1, f_2 of the residue class of f, realising all coefficient bounds. Then, by defining either $g := f_1 - f_2$ or $g := f_2 - f_1$, we obtain a polynomial $g \in I_0$ with $\mathrm{LT}(g) = a\mathbf{x}^\alpha$ and $0 \leq a < \frac{m}{\gcd(m,\alpha!)}$. By Lemma 3.2, we know that $m|_{\mathbb{Z}} a\alpha!$.

We need to show that $a = 0$; so for a contradiction, let us assume that $a > 0$. With $b := \gcd(m, a)$ we still have $m|_{\mathbb{Z}} b\alpha!$, i.e., $\frac{m}{b}|_{\mathbb{Z}}\alpha!$. Then also $\frac{m}{b}|_{\mathbb{Z}} \gcd(m, \alpha!)$ which implies $m|_{\mathbb{Z}} b \cdot \gcd(m, \alpha!)$. But $b \cdot \gcd(m, \alpha!) \leq a \cdot \gcd(m, \alpha!) < m$, yielding the desired contradiction. □

As an immediate consequence, we can count the number of polynomial functions which is the same as the number of residue classes in $(\mathbb{Z}/m[x_1, x_2, \ldots, x_n])/I_0$:

Corollary 3.7. *The number of polynomial functions* $(\mathbb{Z}/m)^n \to \mathbb{Z}/m$ *is given by*

$$N = \prod_{\alpha \in \{0,1,\ldots,m-1\}^n} \frac{m}{\gcd(m, \alpha!)}.$$

In comparison, the number of all functions $(\mathbb{Z}/m)^n \to \mathbb{Z}/m$ equals

$$m^{(m^n)} = \prod_{\alpha \in \{0,1,\ldots,m-1\}^n} m = N \cdot \prod_{\alpha \in \{0,1,\ldots,m-1\}^n} \gcd(m, \alpha!).$$

Hence, if m is not prime, there are much fewer polynomial functions

$\mathbb{Z}/m \longrightarrow \mathbb{Z}/m$	No. of functions	No. of polynomial functions
$m = 2^2$	256	64
$m = 2^8$	10^{616}	10^{16}
$m = 2^{16}$	10^{315652}	10^{52}
$m = 2^{32}$	$10^{41373247567}$	10^{184}

$(\mathbb{Z}/m)^n \to \mathbb{Z}/m$ than functions. This has the consequence that not every problem which can be modelled by functions, like problems coming from formal

verification, can be modelled by polynomials over $\mathbb{Z}/m$ (cf. [12] where, nevertheless, polynomial ideals over $\mathbb{Z}/2^k$ have been used successfully).

Following the idea in the proof of Proposition 3.6, we are able to present a very fast algorithm for computing the reduced normal form, that is, the unique representative of a residue class in the ring $\mathbb{Z}/m[x_1, x_2, \ldots, x_n]$ module I_0. (see [8] for $\mathbb{Z}/2^k$):

Algorithm 1 Reduced normal form in $\mathbb{Z}/m[x_1, x_2, \ldots, x_n]$ with respect to I_0

Input: $f \in \mathbb{Z}/m[x_1, x_2, \ldots, x_n]$ a polynomial, $>$ any monomial order on $\mathbb{Z}/m[x_1, x_2, \ldots, x_n]$
Output: h the reduced normal form of f with respect to I_0
  $h := 0$
  while $f \neq 0$ **do**
    $a\mathbf{x}^\alpha := \text{LT}(f)$
    $c := \frac{m}{\gcd(m, \alpha!)}$
    solve $a = k \cdot c + r$ with $k \in \mathbb{N}$ and $0 \leq r < c$
    $h := h + r\mathbf{x}^\alpha$
    $f := f - k \cdot p_{\alpha,c} - r\mathbf{x}^\alpha$
  end while
  return h

Note that the algorithm makes sure that $f + h$ will always represent the same residue class, as $p_{\alpha,c} \in I_0$. Since initially $h = 0$, this class must be the residue class of f. After termination, which is ensured by the global order, h consists only of terms with appropriate coefficient bound, i.e., h must be the unique representative as given in Proposition 3.6.

3.4 Computing Minimal Strong Gröbner Bases over Different Rings $\mathbb{Z}/m$

The simple structure of minimal strong Gröbner bases provides us with a recursive means to construct G_m from bases for smaller m. We are especially interested in computing G_M from the elements of the already computed set G_m, where $M = q \cdot m$ with q a prime number. The following pairwise disjoint decomposition of G_M is easy to verify:

$$
\begin{aligned}
G_M = & \{p_{\alpha,a} \mid p_{\alpha,a} \in G_m, (\alpha, a) \in S_M\} \\
& \cup \{p_{\alpha,aq} \mid p_{\alpha,a} \in G_m, (\alpha, aq) \in S_M\} \\
& \cup \{p_{\alpha+\beta,b} \mid p_{\alpha,a} \in G_m, \exists \beta \in B(\alpha, a, q) \ \exists b|_\mathbb{z} M \ : \ (\alpha + \beta, b) \in S_M\},
\end{aligned}
$$

where $B(\alpha, a, q)$ denotes the set of all $\beta \succ (0, 0, \ldots, 0)$ such that $(\alpha+\beta)!$ contains one more prime factor q than $a\alpha!$.

This decomposition says that we may already directly find elements of G_M in G_m. Or, secondly, we may build an element of G_M by multiplying an element of G_m by q. Besides altering the coefficient only, we can also try to enlarge

the exponent vector of some $p_{\alpha,a} \in G_m$ such that the new exponent factorial $(\alpha + \beta)!$ contains one more prime factor q than $a\alpha!$. However, enlarging the exponent may introduce many more divisors of M, so that in general we need to adjust the coefficient. It is easy to see that once a suitable β is found, we can set $b = \frac{M}{\gcd(M,(\alpha+\beta)!)}$. The search for suitable β can obviously be limited to the set defined by the condition $\beta \preceq (q, q, \ldots, q)$, that is, we know a finite superset of $B(\alpha, a, q)$.

In practice, all three cases may occur. The following examples are numbered according to the order in the above decomposition. (The number of variables, n, equals 2.)

Example 3.8.

1. $G_3 \subset G_6$, *since* $3! = 6$ *already contains all necessary factors; see Example 3.4 (and the remark regarding $k = 1$) to recall the elements of G_3.*

2. *With q any prime, we have $p_{(3,0),2} \in G_{12}$ and $p_{(3,0),2\cdot q} \in G_{12\cdot q}$.*

3. *We have $6(x - 1)(x - 2)(y - 1)(y - 2) \in G_{24}$. We try to construct an element in $G_{24\cdot 3}$ by enlarging the product of x and y terms. Since $6 \cdot 2! \cdot 2!$ contains one prime factor 3, we try to move to the target product $(x - 1)(x - 2)(x - 3)(y - 1)(y - 2)(y - 3)$ which realizes one more factor 3 because $3^2 \big|_{\mathbb{Z}} 3! \cdot 3!$. Now $b = \frac{72}{\gcd(72, 3! \cdot 3!)} = 2$ and hence $2(x - 1)(x - 2) \cdot (x - 3)(y - 1)(y - 2)(y - 3) \in G_{72}$.*

The above decomposition of G_M, and the structure of G_q for a prime q as discussed in Example 3.4, give rise to the following algorithm.

Algorithm 2 RecComp(M), Recursive computation of G_M

Input: $M \in \{2, 3, \ldots\}$
Output: G_M
  pick any prime factor q of M
  if $M = q$ **then**
    $A := \{q \cdot e_i \mid 1 \leq i \leq n\}$, where the e_i are the unit vectors in $\mathbb{N}^n$
    $G := \{p_{\alpha,1} \mid \alpha \in A\}$
  else
    $m := M/q$
    $H :=$ RecComp(m)
    $G := \{\,\}$
    for all $p_{\alpha,a} \in H$ **do**
      if $(\alpha, a) \in S_M$ **then**
        $G := G \cup \{p_{\alpha,a}\}$
      else
        $G := G \cup \{p_{\alpha,a \cdot q}\}$
        for all $\beta \in B(\alpha, a, q) \subset \{\beta \mid (0, 0, \ldots, 0) \prec \beta \preceq (q, q, \ldots, q)\}$ **do**
          $b := \frac{M}{\gcd(M,(\alpha+\beta)!)}$
          $G := G \cup \{p_{\alpha+\beta,b}\}$
        end for
      end if
    end for
  end if
  return G

References

[1] W. Adams and P. Loustaunau. An introduction to Gröbner bases. (Graduate studies in mathematics) AMS, 2003.

[2] L. Carlitz. Functions and polynomials (mod p^n). *Acta Arith.*, 9:67–78, 1964.

[3] G.-M. Greuel, G. Pfister, and H. Schönemann. SINGULAR *3.1.0 — A computer algebra system for polynomial computations.* 2009. http://www.singular.uni-kl.de.

[4] L. Halbeisen, N. Hungerbühler, and H. Läuchli. Powers and polynomials in $\mathbb{Z}/m$. *Elem. Math.*, 54:118–129, 1999.

[5] N. Hungerbühler and E. Specker. A generalization of the smarandache function. *Integers: Electronic J. Combinatorial Number Theory*, 6, 2006.

[6] A. J. Kempner. Polynomials and their residue systems. *Amer. Math. Soc. Trans.*, 22:240–266, 1921.

[7] G.-M. Greuel M. Wedler O. Wienand M. Brickenstein, A. Dreyer. New developments in the theory of groebner bases and applications to formal verification. *Journal of Pure and Applied Algebra*, 2008.

[8] N. Shekhar, P. Kalla, F. Enescu, and S. Gopalakrishnan. Equivalence verification of polynomial datapaths with fixed-size bit-vectors using finite ring algebra. In *ICCAD '05: Proceedings of the 2005 IEEE/ACM International conference on Computer-aided design*, pages 291–296, Washington, DC, USA, 2005. IEEE Computer Society.

[9] D. Singmaster. On polynomial functions (mod m). *Journal of Number Theory*, 6:345–352, 1974.

[10] F. Smarandache. A function in the number theory. *Analele Univ. Timisoara, Fascicle 1*, XVIII:79–88, 1980.

[11] O. Wienand. Ph.D. thesis. Kaiserlautern, Germany, In prepration, 2009.

[12] Oliver Wienand, Markus Wedler, Dominik Stoffel, Wolfgang Kunz, and Gert-Martin Greuel. An algebraic approach for proving data correctness in arithmetic data paths. In *CAV '08: Proceedings of the 20th international conference on Computer Aided Verification*, pages 473–486, Berlin, Heidelberg, 2008. Springer-Verlag.